2008-06

Prioritizing assets in critical infrastructure systems

Blanco, Hilda

Prioritizing assets in critical infrastructure systems

Dr. Hilda Blanco
Professor and Chair
Department of Urban Design and Planning
University of Washington
hblanco@u.washington.edu

Abstract

Prioritizing is a fundamental task in capital facilities planning and finance. The protection of critical infrastructure systems, essential systems that underpin our society's "national defense, economic prosperity and quality of life" (President's Commission 1997), challenges the traditional methods used for prioritizing capital projects. The critical infrastructure systems identified in the various homeland security official documents are vast and complex systems which include among others, transportation, water supply, telecommunications[1]. The national interest in these systems is clear, protecting these systems from "incapacity or destruction". In effect, the national interest in these systems is to ensure that these systems are resilient and less vulnerable to potential threats, disasters, or accidents. The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (Office of the President 2003) requires government agencies as well as the private sector to identify and prioritize assets most essential to the nation's economic and social well-being. Traditional methods for prioritizing or selecting capital projects for investment fall into two categories, economic evaluation methods and more multicriteria approaches based on expert or departmental judgments, broad categories of need, urgency of need criteria, or program priorities, or goals. (Vogt 2004) Although the multicriteria methods could be applied to prioritize investments in critical infrastructures, such methods are difficult to apply to vast and complex systems often national in scale, and do not necessarily capture the systems or network aspects of the projects. In this paper, I first review and discuss major approaches to prioritization. I then focus on prioritizing system components and networks of critical infrastructures, focusing on Lewis's network theory (2006) approach to prioritize and invest for protection of nodes in critical infrastructure networks, and also review network interdiction approaches. Based on the limitations of the approaches reviewed, the final part argues that an enhanced systems analysis approach based on stock and flow diagrams would retain more information of the systems as systems and as networks than the more abstract network modeling.

.

[1] The following infrastructures have been identified as critical infrastructures for the nation: agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemical industry, postal and shipping. Office of the President. *The National Strategy for Homeland Security,* July 2002.

1. Introduction

Prioritizing is like thinking, everybody thinks they know how to do it, and, in the ordinary sense, we all do know. The issue for policy professionals who engage in this task is to set out and justify the rules or procedures we use to carry out this process on behalf of governments or corporate entities. Granted that each of us knows how to prioritize for ourselves, but how should public agencies or professionals working in such agencies prioritize, when faced with national or state or local agendas?

Prioritizing has received considerable professional attention in public policy. Often, prioritizing is seen to be part of the selection and evaluation of projects or programs for capital facilities planning and financing. As such, it is a primary function in public capital facilities planning (Vogt 2004). Since many critical infrastructures are capital facilities, its literature is most relevant.[2] In public finance, prioritizing projects takes the form of either a variant of cost-benefit analysis or more qualitative methods, ranging from experience-based judgment to sets of criteria based, for example, on need, or functional priorities. Often, some combination of such methods is used. These methods are acceptable at the local, state, and national levels to a large extent because the projects they are applied to are relatively well-bounded within a jurisdiction and/or a system. The idea of protecting or reducing the vulnerability of nation-wide critical infrastructures has unbound the process of prioritizing, and may call for more systems-oriented or network oriented approaches.

After a brief discussion of critical infrastructures and their characteristics, the paper reviews major approaches to prioritization, and their shortcomings when applied to critical infrastructure systems. I then focus on prioritizing projects from a critical infrastructure perspective as applied to system components and networks, discuss more systems-oriented quantitative methods and their limitations, focusing on the network theory approach to prioritize and invest for protection of nodes in critical infrastructure networks developed by Ted Lewis at the Naval Post Graduate School (2006), and also reviewing network interdiction approaches. Based on the limitations of the approaches reviewed, the final part argues that an enhanced systems analysis approach based on stock and flow diagrams would retain more information of the systems as systems and networks than the more abstract network analysis.

2. Critical infrastructures

The concept of critical infrastructures is a relatively new concept, defined in *Critical Foundations* (Pres. Commission Report 1997)[3] as *essential services that underpin our society's "national defense, economic prosperity and quality of life*. The report identified the following 8 critical infrastructures: transportation, oil and gas production and storage,

[2] In the field of public health, priority setting for healthcare has also received academic attention (Mullen and Spurgeon 2000; Mullen 2004).

[3] The report is also known as the Marsh report after Robert T. Marsh, the Chair of the President's Commission on Critical Infrastructures Protection that produced the report.

water supply, emergency services, government services, banking and finance, electrical, and telecommunications. This early definition and listing has been expanded over time by several acts and policies. The USA Patriot Act of 2001 defined critical infrastructures as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters"[4]. The 2003 National Strategy for Homeland Security used the Patriot Act's definition, and identified 11 sectors and 5 key assets. Added to the infrastructures identified in *Critical Foundations* were Agriculture and Food, Public Health, Defense Industrial Base, Chemical and Hazardous Materials, and Postal and Shipping. [5] When the Department of Homeland Security was established in 2003, critical infrastructures and key assets protection was one of its five mandates.[6]

What is it about each of these 11 sectors that makes them critical to the operations of the country or "that could be exploited to cause *catastrophic health effects or mass casualties* comparable to those from the use of a *weapon of mass destruction*"[7] [8]? To be more specific, the various definitions have yielded 4 distinct criteria used to determine the inclusion of these infrastructures as critical. The Marsh report yielded two criteria, their essential role in national defense and in the nation's economic security. The Patriot Act added public health and safety. The Homeland Security Act and the President's National Strategy introduced the criterion of national morale. Thus, the four criteria used to identify critical infrastructures and justify their criticality are: essential role in national defense, economic security, health and safety and national morale. More recently, the *National Infrastructure Protection Plan of 2006* (NIPP)provided a framework for

---

[4] Patriot Act Section 1016 Critical Infrastructure Protection Act of 2001, section (e)

[5] Key assets are individual targets whose destruction could cause large-scale injury, or death or demoralize the country. The 5 key assets identified are:

National Monuments and Icons
Nuclear Power Plants
Dams
Government Facilities
Commercial Key Assets (Major skyscrapers)

It is clear that the key assets identified are not infrastructures, most are not vital to the minimum operation of the nation, but they either have great cultural value, their loss would demoralize the country, or, as in the case of nuclear power plants, can create local disasters.

[6] The responsibilities of DHS include: intelligence and warning, border and transportation security, domestic counter-terrorism, critical infrastructures and key assets, defending against catastrophic terrorism, and emergency preparedness and response. 2002 Homeland Security Act.

[7] The Whitehouse, "Homeland Security Presidential Directive/Hspd-7" December 17,2003. http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html

[8] Also useful to understand the justifications for these infrastructures is President Bush's 2003 Presidential Directive/Hspd-7. In this directive, critical infrastructures and key assets targeted for enhancement are those that are vulnerable to terrorist attacks that could: cause "catastrophic health effects or mass casualties comparable to a weapon of mass destruction" (WMD); or impair federal agencies "to perform essential missions, or ensure the public's health and safety"; "undermine State and local governments' capacities to maintain order and deliver minimum essential public services"; damage the private sector's ability to function and deliver essential services; "have a negative effect on the economy through cascading disruption on other critical infrastructures and key assets"; "undermine the public's morale and confidence in our national economic and political institutions".

developing sector specific plans, and outlined a general strategy for managing risk for critical infrastructures. The steps in the Plan's risk management strategy include: setting security goals; identifying assets, systems, networks and functions; assessing risk; prioritizing; implementing protective programs; and measuring effectiveness. Note that the NIPP applies the concept of prioritizing to countermeasures. The NIPP is a general framework and relies on sector-specific plans to make more concrete its goals and objectives, with due flexibility.

Critical infrastructure systems are recognized as being more critical and vulnerable due to their interdependencies, especially their increasing cyber interdependencies. This growing interdependency has increased their vulnerability to breakdown due to normal accidents, natural hazards, or intentional attacks, from terrorists or criminals. The figure below from the National Research Council Report (2002), *Making the Nation Safer*, is a depiction of the interdependencies of critical infrastructures. As you can see, electricity and telecommunications are mediating infrastructures for all the other systems, but the systems have additional interdependencies.[9]

Figure 1. Critical infrastructure interdependencies

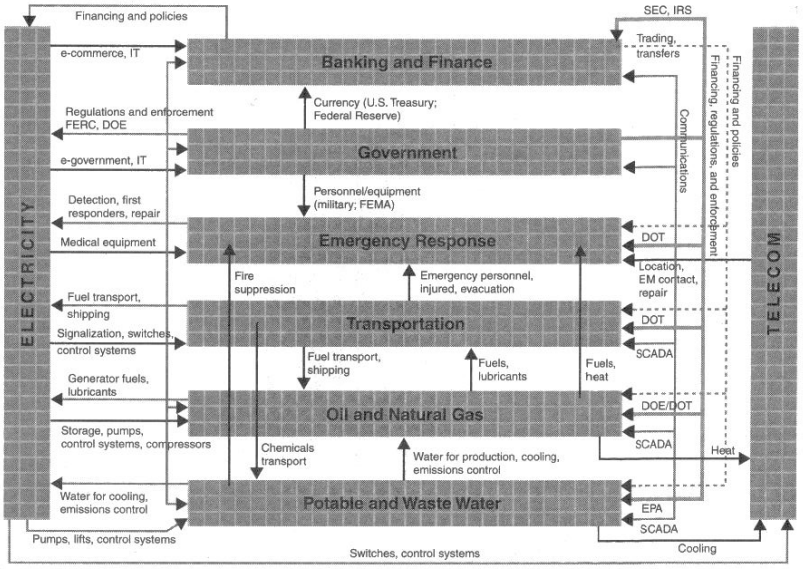


FIGURE 10.4 Critical infrastructure interdependencies. SOURCE: Heller (2002), by permission of the author.

301

Source: National Research Council (2002) p. 301

[9] See also Rinaldi, Peerenboom, and Kelly (2001) for a discussion of critical infrastructure interdependencies.

The difficulty of prioritizing projects in critical infrastructures stems from several reasons. First, critical infrastructures are complex systems. A system is a dynamic set of interdependent elements that interact with each other to produce a result or results. Critical infrastructures are complex systems in that they are composed of various types of elements, including technical or engineered elements, organizational, social, economic, informational, and natural, which interact in complex ways, and are interdependent on one another. They are also so vast, encompassing so many elements over great geographic regions that we cannot hope to protect every part of these systems. For example, in aviation, there are over 500 commercial airports, and close to 19,000 general aviation airports, and approximately 80 commercial carriers, including 14 major carriers (defined by at least $1B in annual operating revenues). Just focusing on commercial flights, U.S. carriers in 2007 made 10.7 million domestic and international flights, and carried 769.4 million persons.(U.S. Department of Transportation 2008) In addition to the airports, and the airplanes and their personnel involved, the aviation system includes a complex air traffic control system, where air traffic controllers who rely on technical equipment as well as human judgment play a crucial role. Many of these systems are national, such as telecommunications, others are large regional systems involving several states, such as power. The vastness of these systems, given limited resources, makes it impossible to be comprehensive in trying to protect them. Instead, we need to be strategic. Note that a critical infrastructure is not just a technical or engineered system, but also includes organizational, economic, and social aspects.

Critical infrastructure systems are complex in themselves, and in their interdependencies. These systems are often what Perrow (1984) called coupled systems, that is, systems with more time-dependent processes (reactions are almost instantaneous); where the sequences are more invariant (for example, in a nuclear or chemical plant, things cannot be added later in the process). Typically, these systems have only one way to reach the production goals (a nuclear plant cannot produce electricity by shifting to coal or oil, but an oil plant can shift to coal); and they have little slack (quantities must be precise, resources cannot be substituted for one another).

As Lewis (2006) argues, we also lack sufficient technical knowledge of these critical infrastructures to understand how to protect them. Complicating this knowledge problem is the interdependency of these systems. As mentioned above, much of the new vulnerability of these systems is due to cyber interdependencies, as well as energy dependencies, which can result in cascading failures. A cascading failure is when a disruption in one infrastructure system causes a failure in the component of another infrastructure system. (Rinaldi, Peerenboom, and Kelly 2001) The 2003 Eastern Blackout is a good example of the interdependencies between the power and water systems and of a cascading failure. Cities like Detroit and Cleveland that relied on pumping for their water supply systems, lost their water supplies during the blackout. And the water systems took twice as long to restore as the power system.

2.1 Protecting Critical Infrastructures

The new public charge to safeguard critical infrastructure systems is, in effect, a charge to reduce the vulnerability of such systems to breakdown. Before 9/11, the vulnerability of critical infrastructure systems made us fear their breakdown due to accidents or natural hazards. After 9-11, the threat of terrorism gained center stage. In the risk analysis literature, risk is defined as severity of impacts times the probability of an event (Lowrance 1976). Vulnerability is often used interchangeably with risk, although there is much ambiguity in the use of the concept. In the hazards literature, vulnerability is often defined as "the susceptibility of resources to negative impacts from hazard events" (NOAA 2008). In the climate change literature, vulnerability has evolved into an integrative concept, and is seen as a function of susceptibility, exposure to a hazard, and adaptive capacity:

> Vulnerability is the degree to which a system is susceptible to, and unable to cope with, adverse effects of climate change, including climate variability and extremes. Vulnerability is a function of the character, magnitude, and rate of climate change and variation to which a system is exposed, its sensitivity, and its adaptive capacity. (IPCC AR4 WG II 2007, 883)

The NIPP (2006, 35) identifies risk as a function of consequence, vulnerability and threat:

$$R = f(C,V,T)$$

where consequence is defined as the negative impacts on public health and safety, the economy, public confidence in institutions and the functioning of governments, etc.; vulnerability is defined as likelihood that an attribute of a component of a system renders it susceptible to fail due to any type of hazard; and threat as the likelihood that a particular asset will suffer an attack or an incident.

The concept of resilience is widely used as the opposite of vulnerability, as the "flip side of vulnerability—a resilient systems or population is not sensitive to climate variability and change and has the capacity to adapt." (IPCC TAR WG II 2001, 89) Four aspects of disaster resilience have been identified (Tierney and Bruneau 2007): a) robustness—the capacity "to withstand disaster forces without significant degradation or loss of performance; b) redundancy—the extent to which there are substitutes to accomplish the function of a system or element of a system, in case a system fails; c) resourcefulness—"the ability to diagnose and prioritize problems and to initiate solutions by identifying and mobilizing material, monetary, informational, technological, and human resources; and d) rapidity—the ability to restore system performance "in a timely way, containing losses and avoiding disruptions."

Prioritizing the critical elements of infrastructure systems to reduce the system's vulnerability to breakdown from natural or intentional causes thus requires identifying their contribution to the system's performance, the major hazards they are exposed to, their susceptibility to specific hazards, and the system's adaptive capacity. Setting priorities for critical infrastructures protection could also be seen as a task to identify the least resilient elements of a system, in which case resiliency could be gauged, following

Tierney and Bruneau, in terms of an element's robustness, the system's or element's redundancy, the resourcefulness or adaptive capacity of the organization or community involved, and the rapidity of restoration.

3. Prioritizing/selection of projects for investment

Traditionally, the major criteria used in capital facilities planning and finance are two, economic efficiency, and public or policy preferences. In consequence, traditional methods used to select projects for planning and budgeting fall into two main categories, economic evaluation methods, and methods that employ multi-criteria and Likert-type scaling measures.

3.1 Economic Selection Methods

The major economic evaluation methods include cost-benefit, net present value, and cost-effectiveness analyses. Cost-benefit analysis is a comparative process that analyzes the potential consequences of several projects, and provides a process for choosing among them. Cost-benefit analysis relies on a prior selection of projects for comparison. It does not provide a rule for identifying projects for comparison. This type of economic evaluation consists of listing the relevant costs and benefits of projects, tangible and intangible, although in practice, it often only includes tangible costs and benefits. In a benefit-cost analysis benefits and costs are translated into monetary terms, and then these benefits and costs are aggregated. Once aggregated, an appropriate discount rate is applied to the total benefits and the total costs. Projects are then compared and the project with the higher benefit/cost ratio is selected. Net present value is benefit-cost analysis without calculating the ratio, the total costs are subtracted from the total benefits for each project and the net present values of the projects are compared. Cost effectiveness is a technique where the benefits or the costs are held constant, and the comparison focuses on the project that provides the most benefits for a set cost, or the most cost-effective project for a given benefit. (Aronson and Schwartz 2004; Stokey and Zeckhouser 1978)

In the context of prioritizing for critical infrastructure systems protection, cost-benefit analysis and other economic evaluation techniques can be useful once an element of a system has been identified as vulnerable. These types of analyses could then be employed to evaluate the economic viability of alternative projects for hardening or making more resilient a specific component in a system. And this is the role that vulnerability assessments of critical infrastructure systems assign to economic evaluation techniques, as we discuss in Section 4 below.

3.2 Multi-criteria Approaches to Prioritizing Capital Projects

Although some local and state governments use economic evaluation methods to select projects, most rely on multi-criteria methods for prioritizing capital projects. (Calia 2001; Vogt 2004; Millar 1988) Criteria typically include government objectives, which are more or less the outcome of representative democracy processes, and thus,

these methods are based on choices concerning public goals. According to Vogt (2004) in his textbook on capital budgeting and finance, these methods range from the experience-based judgments of experts, and departmental priorities set by department heads to the use of rating systems to set priorities for the jurisdiction as a whole based on:

- Broad Categories of Need. In this type of ranking system, projects are rated high or *must do*, medium or *should do*, and low or *could do* priority. A type of need prioritization scheme can also use a numeric or ordinal scale to assign ratings for high, medium and low priorities. (Vogt 2004, 92-94)
- Urgency-of-need criteria—This type of ranking system uses criteria such as: meets legal mandates, removes or reduces a hazard, advances the governing board's goals and objectives, improves efficiency, maintains standard of service, etc. (Vogt 2004, 94-97)
- Weighted rating of urgency-of-need and related criteria—A weighted rating system can also be applied to an urgency-of-need set of criteria, such that each criterion, such as "meets legal mandates" can be rated or scored along a numerical scale from 0 a "clearly no" rating to a 6, a "clearly yes" rating. In addition, each criterion can be assigned a different weight, depending on the priority assigned to the various criteria, e.g., "meets legal mandate" can be assigned a weight of 40%, and the score can then be multiplied by the weight of the criterion, e.g., in the case of a project that meets legal mandates with a score of 5, and a criterion weight of 40%, its weighted score would be 2; while a project that reduces a hazard can be scored a 5, but with a criterion weight of 30%, its weighted score would be 1.5. (Vogt 2004, 97-111)
- Program priorities, goals, and service needs—while "meeting program goals" can be one of several criteria included in the criteria discussed above, some local governments select projects based solely on whether projects meet program priorities, goals and policies of the governing board, which are often expressed in a master plan or strategic plan or the executive's policy agenda. (Vogt 2004, 111-115).

Many of these multi-criteria methods are based on a scaling system, which can be simple or weighted. In such cases, the public facility systems and their performance are reduced to criteria; the criteria are prioritized and sometimes weighted depending on a locality's policy preferences; projects are scored according to the scales used, and their weights are calculated. Capital allocation priorities in a jurisdiction are then decided on the basis of the weighted score assigned to the projects.

4. Multi-criteria approaches for prioritizing in critical infrastructure systems

Prioritization can be applied at several stages in planning processes. The NIPP, for example, outlines a process where prioritizing occurs after risk analysis and is primarily applied to setting priorities for implementation. Calling for prioritization at this stage, and failing to identify the need to prioritize assets ignores the vast nature of infrastructure systems, and the need to prioritize elements prior to vulnerability or risk assessment. The sector-specific plan for water systems identified this issue as a concern and added a component of infrastructure screening to their plan, noting that:

> Given the large number of Water Sector utilities throughout the Nation and the limited resources available to address their security, the objective of the RAMCAP [the NIPP's Risk Assessment Methodology for Critical Assets Protection] process is to prioritize at the national level those sector assets that warrant more in-depth risk analysis. The entire sector, especially owner/operators, may benefit from coordination within the sector on development of a screening process to determine the need for detailed risk assessments. Risk assessments are iterative; therefore, exploring development of screening methodologies could help identify assets that are significant enough to require further assessment. (US DHS and US EPA 2007, 59)

The transportation-specific plan followed NIPP instructions, and applied the concept of prioritization to countermeasures, but the plan also adds a filtering step to assess assets for criticality (2007, 57) right after the development of the asset inventory.

In this article, we are focused on the initial screening of the vast inventories of critical infrastructure systems into a small set of assets or components of a system in order to facilitate further analysis of the vulnerability of such assets to break-down or attack. In this context, several federal and state agencies have turned to multi-criteria scaling systems to identify the most critical components of systems. A good example is the method developed for the American Association of State Highway Transportation Officials (AASHTO) prepared by SAIC (2002) which was developed to assist state departments of transportation (DOT) to prioritize elements of their transportation infrastructures for critical infrastructure protection.

SAIC's guidebook lays out a vulnerability assessment with three major parts: identifying and prioritizing assets or *criticality analysis*; conducting a *vulnerability assessment*; and *post assessment plans*—or planning for implementation of countermeasures. Priority setting is the first part of this process, and it includes identifying all critical assets in the form of a list, establishing and assigning values to critical asset factors, and prioritizing the critical assets, which results in a criticality score for each asset. The second step, conducting the vulnerability assessment, calls for characterizing the threat, identifying exposure level, and scoring the asset vulnerability. This step yields a vulnerability score. The next step calls for the criticality (X coordinates) and vulnerability scores (Y coordinates) for each asset are plotted in a matrix, e.g., if an element of a system has both high criticality and vulnerability scores, it would be plotted in Quadrant I, but if an asset has low criticality and high vulnerability, it would be plotted in Quadrant IV. The final step, the post assessment plans, examines countermeasures to high priority critical assets, and assesses their effectiveness. According to the SAIC handbook, the last step may include conducting cost-benefit analyses and tradeoff studies, as well as actual implementation of countermeasures.

Focusing on the criticality analysis, which establishes priorities, the method begins with a list of assets, which include infrastructure, facilities, equipment, and personnel. The SAIC Guide then provides a list of 14 critical asset factors (the multi-criteria), their value and descriptions for each of the factors. Critical asset factors

include: ability to provide protection, relative vulnerability to attack, casualty risk, emergency response function, functional importance. The factors or criteria are assigned a binary value, which ranges from 1-5 if the factor applies, or 0, if the factor does not apply. The Table below illustrates the method, where each of the letters stands for a criterion or factor. The higher the total score, the more critical the asset.

Table 1. Illustration of SAIC Method for Scoring Criticality of Critical Infrastructure Assets

Critical Asset	Critical Asset Factor														Total Score
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
Asset 1	1	2	5	1	3	3	5	0	5	4	1	5	2	1	38
Asset 2	1	0	5	1	3	3	0	5	5	0	1	0	2	0	26
Asset 3	0	2	0	1	3	3	5	5	5	0	0	5	0	0	29
Asset n	1	2	5	1	3	3	0	0	0	4	1	5	2	0	27

Source: Modified from SAIC Report to AASHTO, A Guide to Highway Vulnerability Assessment (2002), p. 14.

This scoring method is a weighted one, for example, factor or criterion C, the possibility of casualty risk is scored a 5, while factor D, environmental impact, scores a 1, and factor M, functional importance scores a 2. As this illustration makes clear, the value of this approach rests on several things, including, whether the right criteria were included, and whether the appropriate weighing was assigned to each of the criteria. (SAIC 2002, 9-14)

The risk filtering, ranking, and management (RFRM) method developed by Haimes, Kaplan, and Lambert (2002a; Haimes 2004) aims "to identify, prioritize, assess, and manage scenarios of risk to a large-scale system from multiple overlapping perspectives." (Haimes et al. 2002a, 384). It takes into account the multiple perspectives of different stakeholders involved in complex systems and utilizes multicriteria evaluation. It has been applied to filtering over 900 sources of risk to U.S. Army telecommunications systems information assurance (Haimes et al. 2002b), to setting priorities for protecting bridges against terrorist attacks (Leung, Lambert, and Mosenthal 2004) and more recently to protecting critical infrastructure assets in the Army (Anderson, Barker, and Haimes 2008). Although the 8-phase method[10] is focused on risk scenario identification, in their application to Army assets, Anderson and his associates have modified it to apply more directly to assets or elements of systems. The list of critical assets resulting from the Army study is based on two major elements, the criticality of assets to meeting Army goals, and the vulnerability of assets to a particular hazard. RFRM uses a hierarchical holographic model (HHM) to represent the

[10] The eight phases of RFRM are: I) scenario identification through hierarchical holographic modeling (HHM); II) scenario filtering based on scope, temporal domain and level of decision making; III) Bi-criteria filtering and ranking; IV) multicriteria evaluation, criteria related to the system's resilience, robustness, and redundancy; V) quantitative ranking; VI) risk management options are developed and evaluated; VII) safeguarding against missing critical items, continuous review and reevaluation; VIII) operational feedback

characteristics and attributes of a system from multiple aspects, such as Army organization, core competencies, security, challenges, defense and civil infrastructure sectors, geography, temporal, etc. The second step in the process calls for scoping the asset prioritization task. This scoping process is based on a specific threat scenario, e.g., an earthquake, and a specific decision maker, e.g., an Army Material Command Commander, with specified objectives, e.g., deployment readiness, and affected infrastructure sectors, e.g., electrical supply. The commander in such an exercise is concerned with identifying the infrastructure sectors vulnerable to an earthquake that could keep his command from being ready for deployment (Anderson, Barker and Haimes 2008, 7). In the modified RFRM used in the Army study, assets are filtered through the Army's Balanced Scorecard Method (Kaplan and Norton 1992), that is, the set of criteria used to judge critical assets are the core competencies and objectives for the various levels of Army organization.[11]

Assets can then be mapped unto the scorecards. The next step in the method is meant to define the extent to which the assets are required to meet the objectives of the scorecard. This is done through the use of a risk-severity matrix for criticality, based on measures of likelihood and consequence or through an impact matrix, where assets are located in a matrix according to the scorecard objectives they are associated with and the severity of impact they would have on the scorecard objective. For example, in case a risk-severity matrix is used, if loss of Asset 5 is almost certain to cause the failure a scorecard objective, then the element is designated as having high criticality. In case an impact matrix is used, assets with high criticality are assets that have a high impact score and that impact several scorecard objectives.

Unlike the SAIC report, the list generated at this point in the methodology is not ordered or ranked but just bulleted, although in a later step in the process, priority weighting may be added. Similar to the SAIC methodology, the Army study uses the criticality list as input for its vulnerability assessment. Two tools are used in the vulnerability assessment, a risk-severity matrix that is applied to the attributes possessed by an asset, not the asset itself, e.g., throughput, and 14 criteria that relate the ability of a threat scenario to prevail over four defensive properties, resilience, redundancy, robustness, and security. [12] Once the list of vulnerable assets has been produced, an overall prioritized list can be generated by combining the critical asset list with the vulnerable asset list in a matrix, such as depicted in Table 2 below.

Table 2. Modified RFRM Prioritized List of Assets

[11] . This set of criteria corresponds to the prioritizing approach discussed in the section above as the "program priorities of the governing board" approach.

[12] The 14 criteria are: undetectability; uncontrollability; multiple paths to failure; irreversibility; duration of effects; cascading effects; operating environment; wear and tear; hardware/software/human/organization interfaces; complexity and emergent behavior; design maturity; singularity; accessibility; unaffordability.

Vulnerable Asset List	Critical Asset List	
	High	Medium
High	Asset 2, Asset 7	Asset 6
Medium	Asset 4	Asset 9
Low	Asset 1	Asset 3

Source: Modified from Anderson, Barker and Haimes (2008)

The highlighted set of assets identifies the prioritized list of assets. Note here that the criterion for inclusion in the priority list is ranking high in either the critical or the vulnerable asset list. The remaining steps of the RFRM method include risk management, i.e., identifying steps that can be taken to: reduce vulnerability; the trade-offs; and the impacts of current decisions on future options. In addition, RFRM includes feed-back loops to review the findings, as well as to improve the tools.

4.1 Strengths and Weaknesses of Multicriteria Approaches

Multi-criteria approaches are popular for several reasons. They allow stakeholder involvement in the selection of criteria, their scoring and weighting. They do not require extensive calculation, simulation, or modeling, and thus, they make possible widespread application of the criteria by many individuals without much training, since criteria are simple to understand. But as we reviewed above, multi-criteria systems can range from simple, e.g., the SAIC approach, to more complex, e.g., the RFRM approach which requires a large set of inputs. In general, multi-criteria approaches, if standardized across the country, can facilitate comparison across jurisdictions.

Although multi-criteria approaches can be sophisticated, in the analytic process, these methods lose information of the system as a system. Although the RFRM approach emphasizes the importance of the state variables of a system or its components to the concept of vulnerability (Haimes 2006) the interconnectedness of the components of a system is lost in these approaches, as well as the spatial character of critical infrastructure systems. In a similar way, in these methods, criteria can identify interdependence, but they fail to capture the topology of interdependence. Critical infrastructure systems are networks, where there are discernible hubs and connections among hubs. The multi-criteria approaches do not necessarily address the network aspect of these systems.

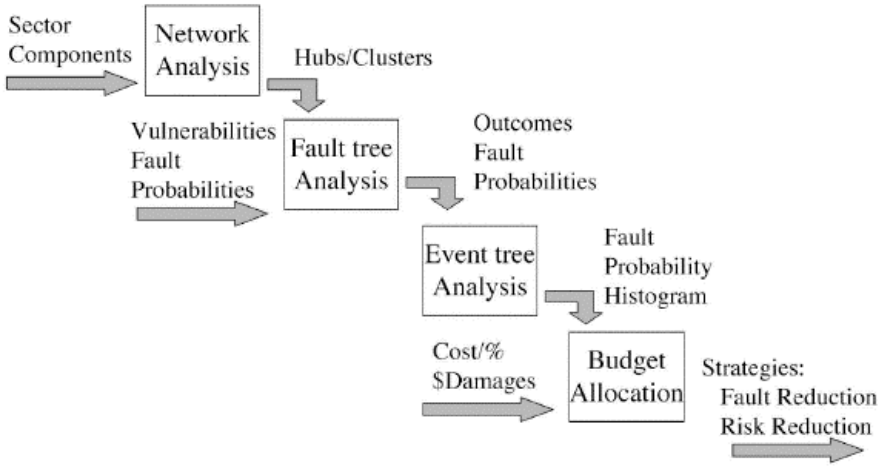
5. Network theory approach applied to critical infrastructures

Ted Lewis (2006) has developed a network theory-based approach to prioritize critical infrastructure components or assets and conduct vulnerability assessments. His text on critical infrastructure protection outlines a vulnerability assessment process, see Figure 1, which includes a network analysis to determine priorities in critical assets within an infrastructure system, followed by fault tree and event tree analyses for the critical assets of a system, and concluding with budget allocation algorithms that can minimize fault or risk. Fault tree and event tree analyses are part of a suite of risk analysis tools used by safety and reliability engineers.

Fault tree analysis is a logical, structured, and graphical process to identify potential causes of system failure. In fault-tree analysis, a logical tree is constructed with the failure of the system at the top of the tree, threats at the bottom, and a chain of causes leading from the threats to the failure connected by logic gates (AND or OR). Event-tree analysis is a logical structured process to determine the consequences of an initiating event and the expected frequency of each consequence. For example, a pipe breaking in a nuclear power station may have many consequences ranging from a very small release of radiation (no significance) up to a very large release of radiation (catastrophic). Event trees model these initiators and consequences, and determine their frequencies. These traditional risk analysis approaches and techniques typically aim to identify all exposures to all components of a system, such as a nuclear power plant, that may be at risk or vulnerable and identify all threats. The results of these analyses then yield probabilistic risks, and depending on the risks the major components that need to be protected are identified.

Since critical infrastructure systems are vast, Lewis's method begins by narrowing down the potential exposures to a few assets of a network. This reduces the assets of a system that need to be analyzed by orders of magnitude, and makes it possible to use the traditional techniques of safety and reliability engineering.[13]

Figure 1. MBVA Process: After Taking Inventory: Perform Network, Fault tree, Event tree Analysis, and Budget Allocation.

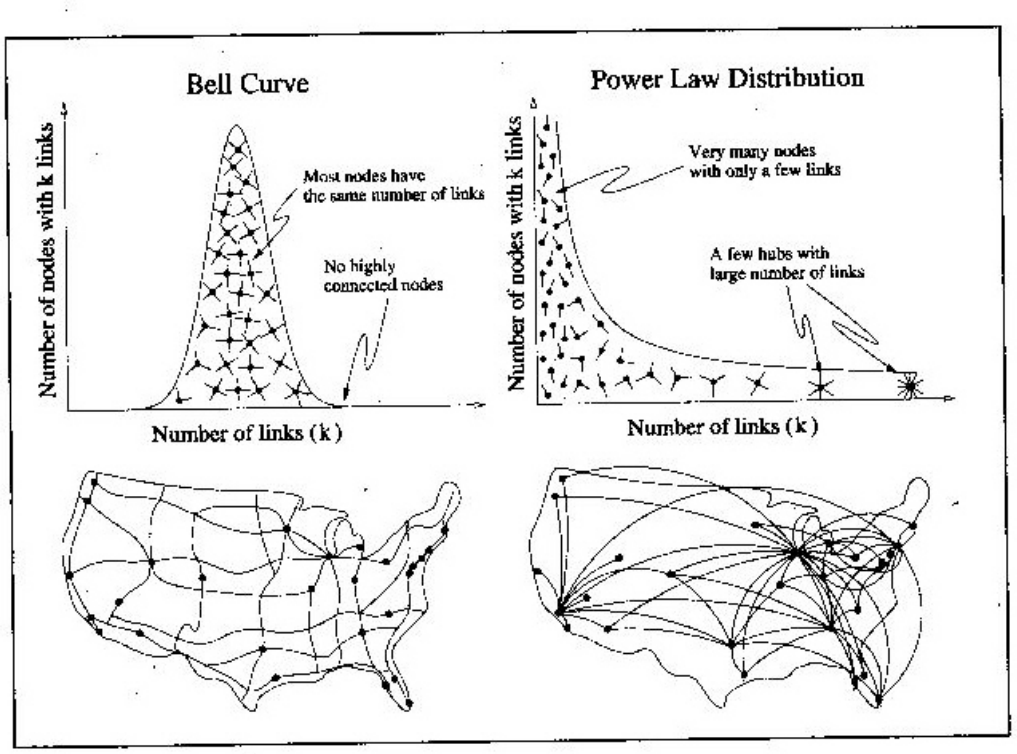


Source: Ted Lewis. 2006. *Critical Infrastructures Protection in Homeland Security*. P. 110. Wiley and Sons.

[13] Notice also, that in addition to the assets identified in the network analysis, key vulnerabilities or threats to such assets as well as the probabilities of the threats occurring are also inputs for the fault tree analysis.

5.1 Using Network Theory to Prioritize Assets in Critical Infrastructure Systems

Lewis's network theory approach is based on recent work on non-random networks, especially scale-free networks (Barabasi 2002) but also small worlds networks (Watts and Strogatz 1998). Network theory is a branch of complexity theory, and initially its focus was on how dynamic, random, non-ordered systems can attain ordered states or self-organization through the application of simple rules. Its mathematical origins date back to Euler's graph theory[14], which modeled systems as nodes and their links to solve topological problems. More recently, since the 1960s, sociologists, such as Milgram (1967), and Granovetter (1973) have revived the use of network theory through algebraic methods. Lewis's work is based on Barabasi's non-random network theory.



Source: A.-L. Barabasi. 2003. *Linked: How Everything is Connected to Everything Else and What it Means for Business, Science, and Everyday Life*. P. 71, PLUME Cambridge, MA

Barabasi's contribution to the mathematical theory of networks, partly through his analysis of the Internet, was to identify a type of network where the linkages are non-random, where just a few hubs have a very high degree of interconnection, and most

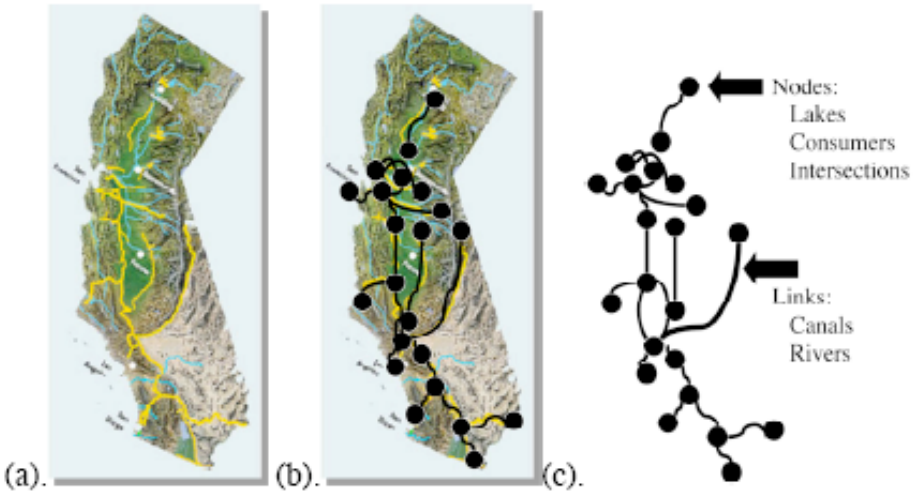
[14] Euler was the foremost mathematician of his time (1707-1783). Euler's inspiration for his invention of graph theory was the popular problem that the 7 bridges of Koningsberg posed to its citizens: Was there a way to start at one of the bridges and cross all of them without crossing anyone twice? Euler's great innovation in 1736 was to graphically portray the land masses as points or nodes and the bridges as links between the nodes. (Barabasi 2002, 9-13; Lewis 2006, 41)

others are sparsely connected in the network. He calls these non-random networks with highly linked hubs, scale-free networks. The figure above compares a random network characterized by a normal distribution of linkages to a scale-free network that is characterized by a power law (that is the histogram drops off quickly as k increases).

Non-random network theory is appropriate for modeling critical infrastructure systems, since these systems typically have a concentration of assets, which can be modeled as critical nodes or hubs, and the distribution of linkages among nodes are non-random, either scale-free or small world. Small world networks are non-random networks whose distributions do not follow a power law. Typically, these are networks with the following characteristics: a large number of nodes; spare, i.e., the average node degree of connection is much smaller than the number of nodes; decentralized, i.e., no dominant nodes; highly clustered—forming neighborhoods; and, connected, i.e., any node can be reached by a finite number of links (Watts 1999).

The application of network theory to a critical infrastructure system provides a simple procedure to determine whether an infrastructure system is random, scale-free, or small world. First, the assets and links between the assets are identified on a map. Then, the assets are characterized as nodes and the linkages as links on the map. In the example Lewis uses of the California aqueduct in the figure below, the nodes are lakes, consumers, and intersections, and the links are canals and rivers. Finally, the mathematical model of nodes and links is transferred to a graph, where the topological features of the links are preserved (3c in the figure).

Figure 2. A Mathematical Graph is used to Model the California Aqueduct as a Network. Map of California Aqueducts, (b). Network Nodes and Links Layered on the California Map, and (c). Network Model of Aqueducts as a Graph.



Source: Ted Lewis. 2006. *Critical Infrastructures Protection in Homeland Security*. P. 80. Wiley and Sons

Once the graph model has been developed for a system, a simple test can be carried out to determine whether a system is random, scale-free or small world network. The test consists of preparing a histogram of the distribution of the degree of linkages for the nodes in the system. If the degree of linkages follows a normal distribution, then the system is random; if it is a power law distribution, then it is a scale-free network; if there are clusters in the distribution, then it is a small world network. This test provides a prima facie rule for prioritizing critical infrastructure assets or components within a system. If a network has a few hubs with a high degree of connectedness, then the system is vulnerable to cascading failures at the nodes. Thus, the network analysis reveals the most critical hubs in the system, where protection and investment measures can best protect the network from cascading failures. Lewis's approach provides convincing simulations of how attacks in different hubs can propagate shutting down the system quickly (see the accompanying software to Lewis's text). As indicated, the network analysis carried out to prioritize hubs is only the first part of Lewis's Model-Based Vulnerability Analysis. Once the critical hubs are identified, fault tree and event tree analyses are carried out for the major threats to such hubs.

The process for identifying the critical nodes in a system is, thus, three-fold: identify the nodes and linkages in a system; graph the nodes and linkages; and, prepare a histogram for the degree of linkage of the hubs. If the histogram reveals a scale-free or small world network, then the critical hubs are the hubs with the greatest degree of linkage. This prioritizing method also has a clear policy directive, i.e., protect the hubs with the greatest degree of linkage. The next section illustrates the method.

5.2 Testing Network Analysis as a Prioritizing Method: The Interstate Highway system as a scale-free network

In his *Critical Infrastructure Protection* text, Lewis analyzes several systems, such as, power, telecommunications, and water in depth using his new method. Although he does not cover transportation in depth, Lewis does discuss its network-like characteristics, and the transportation sector is a good sector to test the method on, since some transportation systems lend themselves easily to such analysis and others do not. Lewis uses the Interstate Highway system as an example to illustrate network analysis, and identifies cities with 6 or more links to the Interstate Highway system. Chicago is the winner with 10 such links, with Indianapolis and Dallas/Fort Worth with 7, and 6 other cities with 6 links. Most major cities have two links, one segment going into the city and another exiting, and the distribution follows more or less a power curve. (Lewis 2006, 90-91)

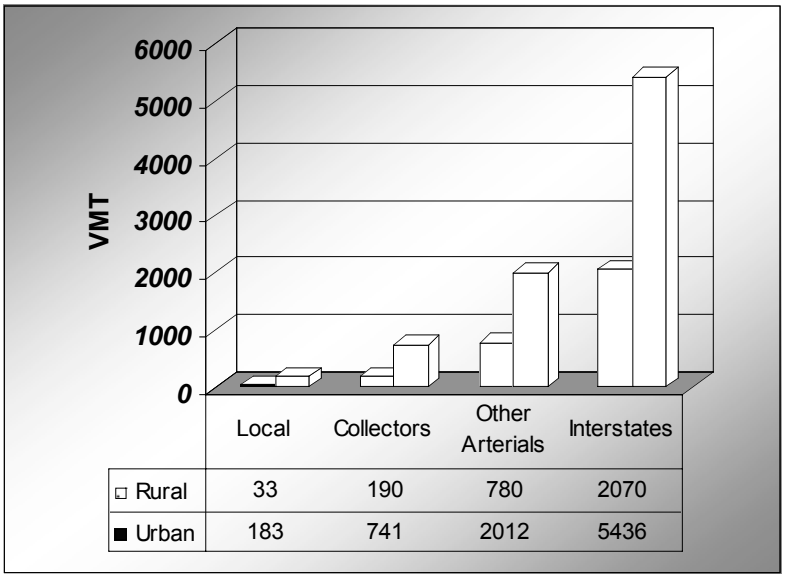
The network analysis methodology applies well to rail systems, because, in rail systems, stations can be interpreted as hubs, and rail lines as connectors. It is a bit more difficult to apply to road systems. What are the nodes in a road system? Lewis points out that segments of roads should at times be interpreted as nodes (Lewis, Chapter 5), but in the Interstate Highway network example above, cities have been interpreted as nodes. In this case, Seattle has four links to Chicago's 10. Does this interpretation lead us to see Chicago as most vulnerable and Seattle as less vulnerable given their degree of

connectedness? Would the method lead us to invest more in protecting the interstate highway system in Chicago than the one in Seattle? But Seattle's lack of redundancy renders it more vulnerable than Chicago. This suggests that the criterion of degree of connectedness used in network analysis needs to be supplemented with a criterion of lack of redundancy. Thus, the choice in interpreting which are to be the nodes versus the links in the network is a crucial choice.

The interstate example also raises the issue of scale, i.e., whether cities can be interpreted as hubs of a highway system. Cities, such as Chicago, are geographically too large, and the 10 interstate highway connections within Chicago are not all concentrated within one segment of road. Within this large city, there are multiple junctures where two to three of the interstate highways are linked. In addition, is it appropriate to consider the interstate highway systems without taking into account the larger road system within a region? The interstate highway system is one element, although a vital one, in regional and national road systems. Within metropolitan areas, they are linked to arterial roads which serve similar functions as the interstate system, and sometimes have similar capacity. In general, in U.S. metropolitan areas, the road system is typically a highly redundant system.

The road system as a whole is an intentional scale-free network, as the histogram of vehicle miles traveled (VMT) per lane mile in the figure below demonstrates. The hierarchical system of road classification, the result of functional and administrative objectives, is the intentional element that makes the road system a scale-free network. This intentional hierarchy of roads leads us to the rule of thumb for road infrastructure, first protect highways, then major arterials. This is one of the major screens that the federal government has used to designate the National Highway System.

Figure 3. Rural and Urban VMT per Lane Mile (in thousands) by Functional Road Class, USA 2003



Source: Adapted from Bureau of Transportation Statistics, Table 1-33. At:
http://www.bts.gov/publications/national_transportation_statistics/2004/html/table_01_33.html

5.2.1 Strengths and weaknesses of Lewis's network theory approach to prioritizing

The major strength of Lewis's network analysis approach to prioritizing is the simple test of node degree it employs for identifying critical hubs in complex networks. This test requires minimal spatial information about a system readily available to designate nodes and links, and the training required to apply such a test is moderate. Also, the graphic display is convincing. Such a test is most useful for scale-free networks, but less so for small world networks (Grubesic et al. 2008). In addition, the software Lewis developed to illustrate his network approach provides convincing simulations of how the network is affected by attacks to different nodes in a system.

Lewis's network analysis approach to prioritizing encounters several challenges, however. Fewer links for transportation or other systems may mean more, rather than less vulnerability. As in the case of the interstate highway connections in Chicago and Seattle, lack of redundancy may trump degree of connectedness. Further, when the node is geographically too large, as in the case of Chicago and the interstate system, the analysis may need to be done at a smaller scale, i.e., to identify vulnerable spots within a node. In general, network analysis at a regional or smaller scale may require subcomponent analysis, such as chokepoints, e.g., tunnels, bridges, vs. entire highway segments. Also, when a system is interconnected with another system, as the interstate highway system is interconnected with local and regional road systems, it may be more strategic to select the more inclusive system to determine priorities.

In critical infrastructures which are supply chains, such as oil or natural gas systems, the sequence or order or direction of flow is important, and the source node or hub may be more critical than the degree of its linkage within a system. For example, in the Southern California Kinder Morgan oil pipeline transmission system, the Watson pipeline is the source pipeline connected to more than 10 refineries in the Los Angeles Basin. Network analysis shows Watson to have two pipeline linkages, while Colton and Niland, internal segments of the pipeline, have 3 linkages. Using a degree of node connectedness indicator would lead us to consider Colton and Niland somewhat more or as critical as Watson[15], yet if Watson were to fail, then the system as a whole would be brought down, whereas if Niland or Colton were to fail, only part of the system would fail. In general, where the connectedness or flow of a system is important, then other network indicators may be necessary to identify network asset priority.

5.3 Interdiction network approaches

[15] Lewis, Chapter 10. Lewis makes up for this by designating a higher value for the Watson pipeline, and a higher damage cost in the fault-event tree analysis. Having to compensate for the lack of guidance from the network analysis indicates that network analysis less useful as a prioritizing tool for this type of system.

Military strategists have used network theory to minimize the disruption or *interdiction* of critical nodes or links in a supply network or chain. When interdiction occurs, the destruction or disabling of a node or critical arc can disrupt the network's topology and performance. Interdiction theory can be used to determine how best to cut off enemy supplies by taking out a small number or the least number of nodes or links from a road, railways, or power grid to disable the network. In the context of critical infrastructure protection, the set interdicted would be the set of assets most vulnerable to attack and in greatest need of protection.

A recent review of network vulnerability interdiction approaches (Grubesic et al. 2008, 90) points out that often, "network facilities are assigned importance to system operability prior to assessing the impacts of a disruption to justify the interdiction scenario examined." Grubesic and colleagues indicate that these priority rankings are based on "simple, graph theoretic measures". Since critical infrastructure systems have such a large set of components, interdiction analysis follows a similar two-step process as the multi-criteria methods we reviewed above. Interdiction analyses first identify important or critical facilities through some graph theoretic measures, and then apply vulnerability assessment to the identified nodes or arcs.

The review discusses two types of indicators of asset importance used in interdiction analysis, global graph theoretic measures, and local network measures. The global indicators summarize overall network structure and enable comparison of networks. They are based on nodes, links, and subgraphs.[16] For example, the Beta index, $\beta = e/v$, where e = the number of edges or links in the graph or network, and v = the number of vertices or nodes in the graph or network, is a simple index of complexity, which can identify whether the network involved has a treelike structure or a circuit network. On the other hand, local network measures are computed for individual links or nodes, and highlight their relative topological features. We have already encountered the simplest local measure of nodal accessibility in Lewis's network analysis, the degree of node. As discussed above, higher degree nodes are assumed to be more critical for system performance. Among other local indicators, the review identifies a local measure of accessibility, T obtained by powering network adjacency relationships C. "Each power n of C represents the number of nodal sequences of length n linking each pair of nodes." (93) This indicator can suggest how proximate a node is to other nodes within a system. The larger the value of T, the more accessible the node. Another indicator of nodal importance is the shortest path between node pairs. Here a smaller path indicates more accessible nodes.(Grubesic et al. 2008, 93-94). Also, recently, a new local network measure to assess network component importance has been proposed by Nagurney and Qiang (2008) which "captures demands, flows, costs and behavior on networks".

Vulnerability assessment in interdiction analyses, according to the review, can be of three types: scenario specific, strategy specific, or structured. A scenario specific study may focus on the impacts of disruptions to a transportation system due to a natural disaster, such as increases in shipment length and cost of transporting goods (Ham, Kim

[16] A subgraph is a subset of a graph, e.g., if a graph represents the regional road system, a subgraph could be a city's in the region road system.

and Boyce 2005). Strategy-specific approaches are characterized by specific node-arc attack strategies, and benefit from the work on scale-free and small world networks already discussed. These approaches simulate the removal of nodes or arcs in specific networks to determine the resulting connectivity of the network. Latora and Marchiori (2005) use this type of approach to assess the most critical nodes or arcs in a network. They test for the redundancy of an asset "by calculating the performance of a disturbed network and comparing it with the original one." (Latora and Marchiori 2005, 015103-1) They found that the more highly connected nodes are not necessarily the most critical. Structured approaches utilize optimization modeling to identify best and worst-case interdiction scenarios. Structured modeling can be focused on several aspects of a network, e.g., network attributes, connectivity, flow or capacity (Grubesic et al. 2008, 95-100). For example, the recent work of Scaparra and Church (2008a,b) involves the development of optimization algorithms for supply systems "to minimize the cost of the or the weighted distance of supplying all demand, where each demand is assigned to its closest facility" . The objective of this research is to identify the subset of assets, which if fortified or hardened, provides the best protection against the worst case loss of the total number of non-fortified facilities. Structured approaches have also developed connectivity and flow optimization interdiction models. (Murray, Matisziw and Grubesic 2007). Optimization modeling typically requires extensive computation, and is opaque to stakeholders.

5.3.1 Strengths and weaknesses of the interdiction approach to prioritizing

The network interdiction approach to prioritizing employs a larger set of indicators than Lewis, both global and local to test for priority. Among these indicators are indicators of connectivity and flow, path length, centrality and betweenness, some of which are more informative than degree of node if the connectivity or flow within a network is important. But such indicators may require real data on flow and performance, which may be difficult to obtain for critical infrastructures. In addition, this type of approach is more opaque to stakeholders, requiring greater mathematical training than other approaches we reviewed.

After reviewing the literature for approaches to interdiction theory, Grubesic et al. apply the various measures they identified in their review to the Abiline Internet system (a U.S. network of internet routers for research universities) for which they obtained empirical data. With respect to identifying critical nodes or arcs, their application revealed that: a) global indicators of importance may provide some insight into the type of system, but are not helpful in identifying critical nodes or arcs in a system; b) the degree of node indicator is not helpful when dealing with a sparse network such as the Abiline system, but other local indicators can be more useful, such as the *T* index of accessibility, which identified the four most critical nodes in the system; and c) even local indicators fail to capture the complexities of nodal importance. They argue that, "parity in a local approach can mask the criticality of nodes in a system, particularly with respect to flow and use" (109). Finally, the authors warn that the criticality of a node or arc cannot be evaluated in an *aspatial* way, without taking into account its location within

the network topology and the possibilities for movement between all other nodes or arcs that remain in the system after a hypothetical attack. (110)

5.5 Prioritizing Critical Infrastructure Assets and Systems Analysis

In this paper, we have reviewed two major multi-criteria approaches to prioritization of critical infrastructure assets, and two types of network analysis, Lewis's network analysis and interdiction theory. As discussed above, both multi-criteria approaches fail to address the infrastructure systems as systems, and their spatial nature. The strength of Lewis's network theory is its computational simplicity and low data requirements. Its application to scale-free networks is insightful, and the accompanying software that models the incapacitation of nodes, and the propagating impacts on a network is a useful tool to educate professionals on network characteristics and cascading failures. However, the approach, as we discussed, faces challenges. Even its application to the Internet, the very system that led Barabasi (2002) to formulate the concept of scale-free networks, has its critics. For example, Doyle and his colleagues (2005, 14501-502) have found that in the Internet, the hubs identified by the greatest degree of linkages are not necessarily the critical nodes. As they argue, systems like the Internet have characteristics that are not captured by network theory, such as protocols and multiple layers of feedback control. They conclude that scale-free network indicators "collapse when faced with real data or when examined by domain experts".

Networks are systems, but they are abstract systems, stripped down to two basic elements, nodes and links. Even the stock-flow diagrams of systems analysis provide more information, and a broader type of systems analysis[17] addresses aspects of a system that are not adequately reflected in either multi-criteria or network approaches. Further, systems analysis is more appropriate for determining the priority of assets in critical infrastructure systems, because determining the criticality of components fundamentally involves understanding the performance of a system. The approaches we reviewed are all concerned with performance, but only systems analysis diagrams aim at outlining how the vital components of a system achieve system performance.

In systems analysis, there are two major tools to model the performance of a complex system, stock and flow and causal loop diagrams. Although causal loop diagrams are more popularly identified with the systems approach, specifically systems dynamics, stock and flow diagrams can retain more information about the flow of a good through a system or the performance of a system. (de Rosnay 1979) For example, in a stock and flow diagram of New York City's water system or an oil transmission system, see Figure 4 below, sources that provide inputs, transmission conduits, valves (that control the volume of flows), reservoir or stock elements, and sinks that receive outputs can be identified. Information flows along the system can also be incorporated into such models. Retaining the information about the role that an asset plays in a system, and where the asset is located in a system is important to determine its criticality. In addition, a stock and flow diagram can depict redundancy or lack of redundancy in a system.

Stock and flow diagrams typically incorporate the capacity of the elements

[17] Such as, an emphasis on the environment of a system, or on performance standards for a system.

involved, but to be more useful for determining the criticality of a component of an infrastructure system, they could be augmented to incorporate the condition of the component, the availability, cost, and rapidity of replacement if disabled, and security measures at the asset level, as well as the protocols or regulations that control the system and component functioning. Hypertext or a simplified geographic information system can be used to add more functionality to the standard stock and flow diagram by enabling layering of information per component. Layered information would remain spatially embedded per component, and would facilitate identifying various aspects of resilience, including levels of robustness, redundancy, resources available in case of a component failure, as well as the rapidity of restoring component function. Prioritization of components could then be based on the resilience of system components, and the extent of flow or processing provided by the component. For example, old aqueduct segments in Upstate New York and old water mains running under Manhattan could both be in similar poor condition, but the old aqueduct segment would be likely prioritized because of its greater flow capacity and location in the system. However, if adequate reservoir conditions obtain near the city, and if the rapidity in which such an aqueduct segment can be repaired in upstate New York outweighs the magnitude of disruption, time delays and cost to repair a major water main break in mid-Manhattan, then the replacement of old water mains in mid-Manhattan could receive a higher priority. Of course, this systems approach to prioritization would involve much analytical work, including some ranking of resiliency criteria. However, the analytical work would be useful for system maintenance, traditional resource allocation, as well as critical infrastructure protection. Further, the basic stock and flow diagram is a simple conceptual model which can be useful in making decisions that involve multiple stakeholders. It provides a handy mental model that incorporates more system-specific information than network models.

In addition, systems models can be interlinked to indicate interdependence. A national effort to model the nation's critical infrastructure interdependencies has already been launched (Min et al. 2007) and the researchers at the national labs leading the effort are using a combination of system dynamics causal feedback loop and Integrated Definition Methods (IDEF) diagrams to model system interdependencies.

6. Conclusion

Recent national policies and plans mandate the protection of critical infrastructure systems. The mandate to protect is interpreted as the need to make less vulnerable or more resilient the vital systems on which we all depend. Resource constraints and the vastness of these systems, which are often comprise thousands of assets or components, challenge the traditional resource allocation methods employed by public finance to prioritize projects. Traditional economic evaluation methods, such as cost-benefit or cost-effectiveness methods, are only appropriate after system assets or components have been prioritized and narrowed down to a few. Multi-criteria approaches to prioritization have been adapted to apply to critical infrastructure systems. But these approaches fail to appropriately capture the systemic and network characteristics of such systems. While Lewis's network theory and interdiction network analyses are important tools which can capture important network characteristics of critical infrastructure components, they also

face challenges and limitations. To address some of these challenges, this paper proposes the use of systems analysis, in particular, the use of enhanced stock and flow diagrams which could retain the network attributes of a system, and yet provide more information on the function of components in such systems. Such an approach would also have the capacity to indicate interdependencies among systems.

References

Anderson, Christopher W., Kash Barker and Yacov Y. Haimes. 2008. Assessing and Prioritizing Critical Assets for the United States Army with a Modified RFRM Methodology. *Journal of Homeland Security and Emergency Management*. 5(1) web page.

Aronson, J. Richard and Eli Schwartz. 2004. Chapter 6. Cost-benefit analysis and the capital budget. In *Management Policies in Local Government Finance*. Editors, J. Richard Aronson and Eli Schwartz. Washington, D. C.: ICMA Press.

Barabasi, A.-L. 2003. *Linked: How Everything is Connected to Everything Else and What it Means for Business, Science, and Everyday Life.* PLUME Cambridge, MA

Calia, Roland. 2001. Priority-setting Models for Public Budgeting. Government Finance Officers Association

De Rosnay, Joel. 1979. *The Macroscope*. New York: Harper and Row. Accessible at: http://pespmc1.vub.ac.be/MACRBOOK.html

Doyle, J. C., D.L. Anderson, L. Li, S. Low, M. Roughan, S. Shalunov, R. Tanaka, and W. Willinger. 2005. The "robust yet fragile" nature of the Internet. *Proceedings of the National Academy of Sciences*. http:www.pnas.org/cgi/doi/10/1073/pnas.0501426102.

Granovetter, Mark. 1973.The Strength of Weak Ties. *American Journal of Sociology*, 78(6), 1360-1380 (1973).

Grubesic, Tony H., Timothy C. Matisziw, Alan T. Murray, and Diane Snediker. 2008. Comparative Approaches for Assessing Network Vulnerability. *International Regional Science Review*. 31(1) 88-112.

Haimes, Y.Y. 2004. *Risk Modeling, Assessment, and Management*. 2nd Edition. Hoboken, New Jersey: Wiley.

Haimes, Y.Y. 2006. On the Definition of Vulnerabilities in Measuring Risks to Infrastructures. *Risk Analysis*, 26(2): 293-296.

Haimes, Y.Y., S. Kaplan, and J.H. Lambert. 2002a. Risk filtering, ranking, and management framework using hierarchical holographic modeling. *Risk Analysis*. 22(2): 381-395.

Haimes, Y.Y., T.A. Longstaff, and G.A. Lamm. 2002b. Balancing Promise and

Risk with Information Assurance in Joint Vision 2020. *Military Operations Research*. 7(3): 31-46.

International Panel on Climate Change (IPCC). 2007. *Climate Change 2007- Impacts Adaptation and Vulnerability.* Contibution of Working Group II to the Fourth Assessment Report of the IPCC.

IPCC. 2001. *Climate Change 2001. Overview of Impacts, Adaptation, and Vulnerability to Climate Change*. Working Group II Contribution to the Third Assessment Report of the International Panel on Climate Change.

Kaplan, R.S. and D.P. Norton. 1992. The Balanced Scorecard – Measures that Drive Performance. *Harvard Business Review*, Jan./Feb.: 71-79.

Latora, Vito, and Massimo Marchiori. 2005. Vulnerability and protection of infrastructure networks. *Physical Review* E71, 015103-1-4.

Leung, M., J.H. Lambert, and A. Mosenthal. 2004. A Risk-Based Approach to Setting Priorities in Protecting Bridges Against Terrorist Attacks. *Risk Analysis*, 24(4): 963-984.

Lewis, Ted. 2006. *Critical Infrastructures Protection in Homeland Security*. Hoboken, NJ: Wiley and Sons

Lowrance, W.W. 1976. *Of Acceptable Risk: Science and Determination of Safety.* Los Altos, CA: William Kaufman, Inc.

Milgram, S.1967. The small world problem. *Psychology today* 2, 60-67.

Millar, Annie. 1988. Selecting Capital Investment Projects for Local Governments. *Public Budgeting and Finance*. Autumn 1988, p. 63-77.

Min, Hyeung-Sik J., Walter Beyeler, Theresa Brown, Young Jun Son, and Albert T. Jones. 2007. Toward modeling and simulation of critical national infrastructure interdependencies. *IIE Transactions* 39, 57-71.

Mullen, Penelope M. 2004. Quantifying priorities in healthcare: transparency or illusion? *Health Services Management Research*. February 2004, 17(1): 47-58.

Mullen, Penelope M. and P. Spurgeon. 2000. Priority Setting and the Public. Oxon: Radcliffe Medical Press, 2000.

Murray, A.T., T.C. Matisziw, and T.H. Grubesic. 2007. Critical network infrastructure analysis: Interdiction and system flow. *Journal of Geographical Systems* 9: 103-117.

Nagourney, Anna and Qiang Qiang. 2008. A network efficiency measure with application to critical infrastructure networks. *Journal of Global Optimization*. 40:261-275.

National Oceanic and Atmospheric Administration (NOAA) Coastal Services Center, Community Vulnerability Assessment Tool.
http://www.csc.noaa.gov/products/nchaz/htm/tut.htm

National Research Council. 2002. *Making the Nation Safer.* National Research Council.

Office of the President. 2002. *The National Strategy for Homeland Security,* July 2002.

Office of the President. 2003. The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets. February, 2003.

Office of the President. 2003. Homeland Security Presidential Directive (HSPD-7) December 17,2003.
http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html

Perrow, Charles. 1984. *Normal Accidents*. New York: Basic Books.

President's Commission on Critical Infrastructure Protection (PCCIP). 1997. *Critical Foundations: Protecting America's Infrastructures. The Report of the President's Commission on Critical Infrastructure Protection.* Washington D.C.
http://handle.dtic.mil/100.2/ADA331523

Rinaldi, Steven M., James P. Peerenboom, and Terrence K. Kelly. 2001. Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine*. Pp. 11-25. December 2001.

Scaparra, Maria and Richard L. Church. 2008a. A bi-level mixed-integer program for critical infrastructure protection planning. *Computers and Operations Research* 35: 1905-1923.

Scaparra, Maria and Richard L. Church. 2008. An exact solution approach for the interdiction median problem with fortification. *European Journal of Operational Research*. 189: 76-92.

Science Applications International Corporation (SAIC). 2002. *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection*. Prepared for The American Association of State Highway and Transportation Officials' Security Task Force. May 2002. Vienna, VA.

Stokey, Edith and Richard Seckhouser. 1978. *A Primer for Policy Analysis*. NY: W.W. Norton and Co.

Tierney, Kathleen and Michel Bruneau. 2007. Conceptualizing and Measuring Resilience. A Key to Disaster Loss Reduction. *TR News*. May-June 2007. 250:14-17.

U.S. Department of Homeland Security. 2006. *National Infrastructure Protection Plan.* http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm#1

U.S. Department of Homeland Security and US Environmental Protection Agency. 2007. *Water. Critical Infrastructure and Key Resources. Sector-Specific Plan as Input to the National Infrastructure Protection Plan.* May 2007. Accessed at http://www.michigan.gov/documents/deq/deq-wb-wws-Water_SSP_5_21_230463_7.pdf

U.S. Department of Homeland Security, Transportation Security Administration. 2007. *Transportation.. Critical Infrastructure and Key Resources. Sector-Specific Plan as Input to the National Infrastructure Protection Plan.* May 2007. Accessed at http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation.pdf

U.S. Department of Transportation, Research and Innovative Technology Administration, Bureau of Transportation Statistics. Press release, March 13, 2008. December 2007 Airline Traffic Data. Found at: http://www.bts.gov/press_releases/2008/bts013_08/html/bts013_08.html

U.S. Patriot Act of 2001. Section 1016 Critical Infrastructure Protection Act of 2001, section (e)

Vogt, John A. 2004. *Capital Budgeting and Finance: A Guide for Local Governments*. Chapter 4. Prioritizing Capital Projects pp. 89-118. ICMA

Watts, D. 1999. Networks, Dynamics, and the Small-World Phenomenon. *American Journal of Sociology*. 105(2): 493-527. Sept. 1999.

Watts, D. and S.H. Strogatz. 1998. Collective Dynamics of 'small world' networks. *Nature.* 393:440-42